

## UNITED STATES DISTRICT COURT

for the  
District of OregonIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)2199 Union Avenue, Apt. 1,  
North Bend, Oregon 97459

Case No. 6:17-MC- 552

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

2199 Union Avenue, Apt. 1, North Bend, Oregon 97459 as described in Attachment A hereto.

located in the \_\_\_\_\_ District of \_\_\_\_\_ Oregon \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 U.S.C. § 2252AOffense Description  
Transportation, distribution, receipt, and possession of child pornography


The application is based on these facts:  
See affidavit which is attached hereto and incorporated herein by this reference.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signatureMiguel A. Perez, Special Agent, FBI  
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/2/2017

  
Judge's signature

City and state: Eugene, Oregon

Jolie A. Russo, United States Magistrate Judge  
Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF MIGUEL A. PEREZ

**Affidavit in Support of an Application  
Under Rule 41 for a Search Warrant**

I, Miguel A. Perez, being duly sworn, do hereby depose and state as follows:

**Introduction and Agent Background**

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been since January 2015. I am currently assigned to the Portland Division at the Eugene, Oregon Resident Agency. During my training in the FBI Academy in Quantico, Virginia, I received training in a variety of investigative and legal matters, including the topics of Fourth Amendment Searches and probable cause. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252A, and I am authorized by the Attorney General to request a search warrant

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 2199 Union Avenue Apt 1, North Bend, Oregon 97459 (hereinafter "Premises"), as described in Attachment A hereto, for evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252A, involving the transportation, distribution, receipt, and possession of child pornography. As set forth below, I have probable cause to believe that such property and items, as described in Attachment B hereto, including any digital devices or electronic storage media, are currently located at 2199 Union Avenue Apt 1, North Bend, Oregon 97459.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement

officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

#### **Applicable Law**

4. Title 18, United States Code, Section § 2252A (a)(1) makes it a crime to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer. Section 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means or facility, including by computer. Title 18, United States Code, Section 2252A(a)(5)(B) makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. The term child pornography is defined in Title 18, United States Code, Section 2256(8).

#### **Background on Computers and Child Pornography**

5. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers, computer technology, and the Internet have drastically changed the manner in which child pornography is produced and distributed.

6. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

7. Child pornographers can upload images or video clips directly from a digital camera to a computer. Once uploaded, they can easily be edited, manipulated, copied, and distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer through the use of a scanner. Once uploaded, they too can easily be edited, manipulated, copied, and distributed. A modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

8. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Images and videos of child pornography can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like, many of which are small and highly portable and easily concealed, including on one's person.

9. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs, bulletin board services, e-mail, and "peer-to-peer" (P2P) file sharing programs. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online



storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

10. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in the computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

11. P2P file sharing is a method of communication available to Internet users through the use of special software. The software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers together. There are different software applications that can be used to access these networks, but these applications operate in essentially the same manner.

12. To access a P2P network, a user first obtains the P2P software, which can be downloaded from the Internet. This software is used exclusively for the purpose of sharing digital files. When the P2P software is installed on a computer, the user is directed to specify a "shared" files folder. All files placed in that user's shared folder are available to anyone on the world-wide network for download. Most P2P software gives each user a rating based on the

number of files he/she is contributing to the network. This rating affects the user's ability to download files. The more files a user is sharing, the greater his/her ability is to download files. However, a user is not required to share files to utilize the P2P network.

13. One aspect of P2P file sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time.

14. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer or device during an online session. The IP address provides a unique location making it possible for data to be transferred between computers. An IP address can be statically assigned, meaning it is permanently assigned to a particular user and does not change from one Internet session to another. An IP address may also be dynamically assigned, meaning that a different number may be assigned to a particular user during each Internet session. Regardless of whether an IP address is dynamically or statically assigned, only one computer or device can be assigned a particular IP address at any given time.

15. Third-party software is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

16. I know, based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including people who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such people maintain their collections of child pornography in safe, secure, and

private locations, such as their residence, and on computers and digital storage media under their direct control. Such people often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period of time.

### **Statement of Probable Cause<sup>1</sup>**

17. On June 8, 2017, an FBI Online Covert Employee (OCE) was connected to the Internet and had signed onto a publicly-available P2P file sharing program. The OCE was investigating the sharing of child pornography files on this particular P2P file sharing network. The OCE was located in Spokane, Washington during this online undercover operation.

18. On June 8, 2017, using the P2P program, OCE identified a computer with the IP address 172.223.200.182 port 27450 as offering child pornography files to download over the

---

<sup>1</sup> Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *IP address.* The Internet Protocol address (or simply “IP address”) is a unique numeric address used by digital devices on the Internet. Every digital device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some digital devices have static—that is, long-term—IP addresses, while other digital devices have dynamic—that is, frequently changed—IP addresses.

b. *Internet.* The Internet is a global network of digital devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. *Storage medium.* A storage medium is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

P2P network. While on a computer in Spokane, the OCE downloaded child pornography from IP address 172.223.200.182 on the following days in June 2017: 8<sup>th</sup>, 9<sup>th</sup>, 10<sup>th</sup>, and 11<sup>th</sup>.

19. On August 10, 2017, I conducted a review of the files downloaded during the undercover operation. The files were saved on four Blu-Ray disks labeled "Disk #1, "Disk #2", "Disk #3", and "Disk #4."<sup>2</sup>

20. The disk labeled "Disk #1" contained files that were downloaded on June 8, 2017. Disk #1 contained several images of child erotica and child pornography. An image file of note named "jess and nina" in a folder called "Preteen girls nude pthc lolita underage real!" shows what appears to depict two teen females completely nude on a sofa. One female teen has her mouth opened and on the other female teen's nipple.

21. The disk labeled "Disk #3" contained files that were downloaded on June 9, 2017. Disk #3 contained several images of child erotica and child pornography. A file folder called "Set 08" found in file path "LS Studio|Enjoy the Show|Issue 02 Enjoy the Show|Images|Set 08" contained multiple images that shows what appears to depict two teen females completely nude in a bath tube filled with water. The images show the teen females putting their hands on each others' bodies, exposing their chest/breasts, and their vaginas.

22. The disk labeled "Disk #4" contained files that were downloaded on June 9th, 10th, and 11th 2017. Disk #4 contained several images of child erotica and child pornography. A

---

<sup>2</sup> Pursuant to *United States v. Perkins*, 850 F.3d 1109 (9th Cir. 2017), where the images described are lascivious exhibitions, copies of the images of child pornography described above will be furnished to the United States Magistrate Judge who reviews this affidavit so the Magistrate Judge can determine if they constitute child pornography as defined under federal law. I will retain the images the Magistrate Judge reviews in a sealed envelope through the conclusion of this case, including any appeals.



file of note named "Ihv-030-109" with file path "LS Studio|Hawaiian Breeze|LS Land Issue - #26|Hawaiian Breeze|Ihv-30|Ihv-030-109" contained a mostly naked prepubescent female exposing her vagina. The prepubescent female is lying on her back, wearing heavy make-up around her eyes and on her lips, and her hair is made up. She has a skirt lifted around her stomach and her legs are spread apart exposing her vagina.

23. On June 14, 2017, the OCE served an administrative subpoena to Charter Communications for the IP address 172.223.200.182. Charter Communications responded on June 20, 2017 and provided the following subscriber information during the time frame the downloads occurred:

Subscriber Name: Katie Montoya

Subscriber Address: 2199 Union Avenue Apt 1, North Bend, Oregon 97459

User Name or Features: kmontoyal@charter.net, kirkmcamis@charter.net

Phone Number: (541) 217-9346

24. On August 11, 2017, a Lexis Nexis search conducted of address 2199 Union Avenue Apt 1, North Bend, Oregon 97459 showed Kirk McAmis as living at the subject premise. A search of a law enforcement database for driver's license information for the State of Oregon listed "Kirk Douglas Mc Amis" at address as 2199 Union Avenue Apt 1, North Bend, Oregon 97459. Kirk McAmis has criminal convictions for petty theft, theft of property, theft of a utility service, and battery. A google search showed Kirk McAmis as a local computer technician that gave a class on computers at the Coos Bay Public Library in Oregon.

25. On August 11, 2017, a search of a law enforcement database for driver's license information for the State of Oregon listed "Kathleen Yvonne Montoya" at address 116 D Lee Ln,

Myrtle Creek, Oregon 97457. The driver's license was issued on 10/25/2016. No criminal convictions for Montoya were found during a criminal history search.

26. On August 17, 2017, a law enforcement officer with the North Bend Police Department (NBPD) provided information related to Kirk Douglas McAmis and address 2199 Union Avenue, Apartment 1, North Bend, Oregon. NBPD database shows Kirk McAmis living at the subject address. A NBPD incident report shows Kirk McAmis was mentioned as "Involved/Contacted" in a report made on June 23, 2014, NBPD case number L20142726 for sex abuse. In the report Kathleen Yvonne Montoya reported possible sexual abuse between her father, Kirk McAmis, and his grand-daughter. Kathleen Montoya is the guardian and aunt of the alleged victim. Kathleen Montoya and the granddaughter reported that Kirk McAmis may have moved the grand-daughter's underwear aside exposing her vagina while she was asleep in the living room of his apartment. The granddaughter reported she didn't see or feel her grandfather touching her, but she had been asleep, and that he could have. The granddaughter said she woke up to seeing her grandpa walking around the living room, "acting creepy".

27. McAmis was not charged for the June 23, 2017 incident, because the he NBPD detective determined that the granddaughter did not make any disclosures as to anything criminal during the forensic interview. The Kids' HOPE Center that investigated the incident indicated that the investigation into the incident did not go further because there were credibility issues with the statements made by the granddaughter. A note in the incident report dated October 28, 2014, from a private investigator, states the private investigator interviewed McAmis' granddaughter in October 2014 and she advised that she had made a false sex report against Kirk McAmis on June 23, 2014.

28. On August 17, 2017, I conducted a physical surveillance at 2199 Union Avenue, North Bend, Oregon. A green Dodge with Oregon tag WNP555 was observed parked on the backside of the property. A law enforcement database search showed the Dodge is registered to Kirk McAmis.

29. On August 17, 2017, an open WiFi survey was taken using a Samsung cellphone. All the WiFi networks around the residence appeared to be closed/password protected except for the networked named "HappyMoose-guest".

30. On October 13, 2017, the property manager for the apartments at 2199 Union Avenue, North Bend, Oregon advised Kirk McAmis is renting apartment #1 at 2199 Union Avenue, North Bend, Oregon. The property manager also provided McAmis moved into apartment #1 in April 2014. The property owner pays for water, sewage, and garbage. McAmis pays for electric and internet service. The apartment is a one bedroom and it is approximately 600 square feet. There are four apartments in the house at the 2199 Union Avenue. Three apartments are occupied.

31. 2199 Union Avenue Apt 1, North Bend, Oregon is a two story four-plex residence with a red brick and white siding exterior. Apartment #1 is located on the east side, lower level of the house. The entrance to apartment #1 is on the opposite side of Union Avenue, on the backside of residence. The apartment has a "1" located on the outside of the apartment.

32. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to

as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

33. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know:

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.



c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

d. Based on the conduct here—making child pornography available for download from a computer accessing the internet at the Premises—I am aware that computer equipment was used as part of this crime. Thus, there is reason to believe that there is a computer system currently located on the premises.

34. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the Premises, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This “timeline” information may tend to either inculcate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user’s state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user’s motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a “wiping program” to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to commit a crime to possess, transport, receive and distribute child pornography, the individual's digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain: data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was

achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

35. In most cases, a thorough search of the Premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the Premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems,



application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

36. Because potentially two or more people share the Premises as a residence, it is possible that the Premises will contain digital devices that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those digital devices, the warrant applied for would permit the seizure and review of those items as well.

37. *Nature of the examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

38. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the

warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

39. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

40. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

41. The government may retain the digital device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the digital device and/or the data contained therein.

42. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its

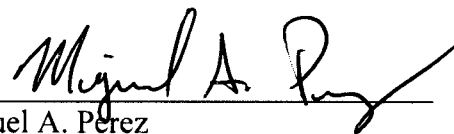
obligations by destroying data or returning it to a third party.

43. The government has made the following prior efforts in other judicial fora to obtain evidence sought under the warrant: Grand jury subpoena and administrative subpoena.

### Conclusion

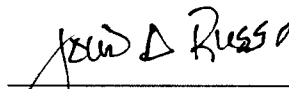
44. Based on the foregoing, I have probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2) and (a)(5)(B), transportation, receipt, distribution, and possession, as described above and in Attachment B, are presently located at 2199 Union Avenue Apt 1, North Bend, Oregon 97459, which is described above and in Attachment A. I therefore request that the Court issue a warrant authorizing a search of the Premises described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

45. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Amy Potter and AUSA Potter advised me that in her opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.



Miguel A. Perez  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me this 2<sup>nd</sup> day of November 2017.



Jolie A. Russo  
United States Magistrate Judge

**ATTACHMENT A**  
**DESCRIPTION OF PREMISES TO BE SEARCHED**

2199 Union Avenue, Apt 1, North Bend, Oregon 97459 is a two story four-plex residence with a red brick and white siding exterior. Apartment #1 is located on the east side, lower level of the house. The entrance to apartment #1 is on the opposite side of Union Avenue, on the backside of residence. The apartment has a "1" located on the outside of the apartment.





## **ATTACHMENT B**

### **Items to Be Seized**

The items to be searched for, seized, and examined, are those items on the premises located at 2199 Union Avenue Apt 1, North Bend, Oregon 97459, referenced in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), transportation, receipt, distribution, and possession of child pornography. The items to be seized cover the period through the date of the execution of the search warrant.

1. The items referenced above to be searched for, seized, and examined are as follows:

a. Any and all records, documents, or materials, including correspondence, that pertain to the production, possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

b. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

c. Any and all motion picture films, video cassettes, and digital video disks ("DVDs") of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

d. Any and all records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by United States mail or by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

e. Any and all records, documents, or materials relating to the production, reproduction, receipt, shipment, trades, purchases, or transactions of any kind involving the transmission, through interstate commerce (including by United States mail or by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

f. Any and all records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

g. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage media, including CDs or DVDs.

h. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, receiving, or transporting child pornography, including chat logs, call logs, address book or contact list entries, digital images sent or received, and the like.

i. Computers, storage media, or digital devices used as a means to commit the violations or that are capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband or evidence, fruits, or instrumentalities of such crimes, including transporting, receiving, distributing, possessing, and accessing with intent to view child pornography in violation of 18 U.S.C. § 2252A (a)(1), (a)(2) and (a)(5)(B).

j. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, web cams, microphones, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined above, or to create, access, process, or store the types of contraband, or evidence, fruits, or instrumentalities of such crimes, as set forth herein;

k. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, iPods, iPads, tablets, and cellular telephones capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband or evidence, fruits, or instrumentalities of such crimes, as set forth herein;

2. As used in this attachment, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been

created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter “Computer”):

- a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence.
- b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.
- c. Evidence of the lack of such malicious software.
- d. Evidence indicating how and when the Computer was accessed or used to



determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.

e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation.

f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.

h. Evidence of the times the Computer was used.

i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.

j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.

k. Records of or information about Internet Protocol addresses used by the Computer.

l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

n. Routers, modems, and network equipment used to connect computers to the Internet.

### **Search Procedure**

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

8. The government may retain the computer and storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

9. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

**UNITED STATES DISTRICT COURT  
DISTRICT OF OREGON  
EUGENE DIVISION**

*In the Matter of the Search of:*

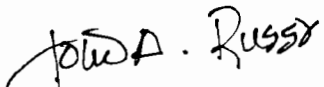
Case No. 6:17-<sup>mc</sup>~~cr~~-552

2199 Union Avenue Apt 1, North Bend,  
Oregon 97459

**CHILD PORNOGRAPHY SUBMITTED FOR REVIEW  
BY UNITED STATES MAGISTRATE JUDGE**

I have reviewed the contents of this envelope, which consists of four images, and I find that they constitute child pornography as defined by federal law. The applicant is directed to maintain custody of the envelope and its contents in a secure location through the conclusion of the investigation and any resulting prosecution, including any appeals.

DATED this 2<sup>nd</sup> day of November 2017.

  
\_\_\_\_\_  
HONORABLE JOLIE RUSSO  
United States Magistrate Judge